



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,055	12/14/2001	Keith L. Shippy	884.602US1	6579

7590 06/29/2005

Sharmini N. Green  
c/o BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP  
12400 Wilshire Boulevard  
Seventh Floor  
Los Angeles, CA 90025

EXAMINER

DINH, KHANH Q

ART UNIT PAPER NUMBER

2151

DATE MAILED: 06/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

10/017,055

Applicant(s)

SHIPPY ET AL.

Examiner

Khanh Dinh

Art Unit

2151

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 14 December 2001.  
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-33 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

1. Claims 1-33 are presented for examination.

***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 2, 7 and 9-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Ishida et al.; (Publication number US-2001/0032258 A1) (hereafter Ishida).

As to claim 1, Ishida discloses a system for detecting and deterring rollback attacks, comprising:

a variable time period (VTP) (time of access), a time duration to a next connection (TDNC) and an access log (using URL access log, see fig.1, Paragraph (para). [0075] to para [0078]);

a server (update server s9 fig.1) to transmit the variable time period (VTP) and the time duration to the next connection (TDNC) and to verify the access log (storing access information from clients at the update server, see para [0079] to para [0083]);  
and

a client to update the access log approximately every variable time period

(VTP) and to connect to the server approximately after the time duration to the next connection (TDNC) (see fig.6, para [0086] to para [0093] and para [0097] to para [0102]).

As to claim 2, Ishida discloses the client is a personal computer (PC) (user terminal 4 fig.1) (see [0071] to [0074]).

As to claim 7, Ishida further discloses a media content provider (see para [0137] to [0145] and [0150] to [0154]).

As to claim 9, Ishida further discloses the access log is used for billing (see para [0096] to [0102] and [0107] to [0119]).

As to claim 10, Ishida discloses a method for detecting and deterring rollback attacks, comprising:

- establishing a shared secret between a client and a server and transmitting, by the server to the client, a variable time period (VTP) and a time duration to a next connection (TDNC) (using URL access log, see fig.1, Paragraph (para) [0075] to para [0078]).

- updating, by the client, an access log approximately every variable time period (VTP) and initiating, by the client to the server, a connection approximately after the

Art Unit: 2151

time duration to the next connection (TDNC) (storing access information from clients at the update server, see para [0079] to para [0083]);

transmitting, by the client to the server, the access log and verifying, by the server, the access log (see fig.6, para [0086] to para [0093] and para [0097] to para [0102]).

As to claim 11, Ishida discloses establishing a new shared secret between the client and the server each time the client connects to the server (see fig.9, [0086] to [0093] and 0096] to [0102]).

As to claims 12 and 13, Ishida discloses establishing a new variable time period (VTP) and a new time duration to a next connection (TDNC) each time the client connects to the server and incrementing, by the client, a counter, after each update to the access log (see fig.9, [0086] to [0093] and 0096] to [0102]).

As to claims 14 and 15, Ishida discloses automatically detecting an anomaly and decreasing the variable time period (VTP), upon detecting an anomaly (see [0086] to [0093] and [0130] to [0145]).

As to claims 16 and 17, Ishida discloses decreasing the time duration to a next connection (TDNC), upon detecting an anomaly and encrypting the access log (see [0086] to [0093] and [0130] to [0145]).

As to claims 18 and 19, Ishida discloses each entry in the access log is encrypted and the access log is re-created each time the client connects to the server (see [0097] to [0109] and [0130] to [0145]).

As to claim 20, Ishida discloses a machine for detecting and deterring rollback attacks, comprising:

- a processor (s9 fig.1) and a storage device (16 fig.1) coupled to the processor;
- a background component storable on the storage device and executable on the processor to update an access log approximately every variable time period (VTP) (using URL access log, see fig.1, Paragraph (para) [0075] to para [0078]);
- a content player component storable on the storage device and executable on the processor to update the access log to indicate content provided (storing access information from clients at the update server, see para [0079] to para [0083]);

Claims 21 and 22 are rejected for the same reasons set forth in claims 17 and 18 respectively.

As to claims 23 and 24, Ishida discloses a communication component capable of connecting to a server approximately after a time duration to a next connection (TDNC) and transmitting the access log (see fig.9, [0086] to [0093] and 0096] to [0102]).

Art Unit: 2151

As to claim 25, Ishida discloses receiving a new variable time period (VTP) and a new time duration to the next connection (TDNC) (see [0086] to [0093] and [0130] to [0145]).

As to claims 26 and 27, Ishida discloses the communication component is capable of receiving a new access log and decrypting the new access log (see [0086] to [0093] and [0130] to [0145]).

As to claim 28, Ishida discloses a machine-accessible medium having associated content capable of directing the machine to perform a method of detecting and deterring rollback attacks, the method comprising:

transmitting, by a sender (user terminal 4 fig.1), a new access log (using URL access log, see fig.1, Paragraph (para) [0075] to para [0078]);

transmitting, by the server (s9 fig.1), a new variable time period (VTP) and a new time duration to the next connection (TDNC) (storing access information from clients at the update server, see para [0079] to para [0083]);

As to claim 29, Ishida discloses receiving, by the server, an old access log and inspecting, by the server, the old access log (see fig.9, [0086] to [0093] and [0096] to [0102]).

As to claim 30, Ishida discloses establishing, by the server, a shared secret with a client (user), decrypting, by the server (update server s9 fig.1), the access log and encrypting,

Art Unit: 2151

by the server, the new access log; and encrypting, by the server, the new variable time period (VTP) and the new time duration to the next connection (TDNC) (see [0086] to [0093] and [0130] to [0145]).

As to claim 31, Ishida discloses: initiating, by a client, a connection with the server; transmitting, by the client, the access log to the server [0096] to [0102];

receiving, by the client, the new access log and receiving (using access information), by the client, the new variable time period (VTP) and the new time duration to the next connection (TDNC); and storing, by the client, the new access log, the new variable time period (VTP), and the new time duration to the next connection (TDNC) (see [0086] to [0093] and [0130] to [0145]).

As to claim 32, Ishida discloses establishing, by a client, a shared secret with the server; encrypting, by the client, the access log; decrypting, by the client, the new access log; and decrypting, by the client, the new variable time period (VTP) and the new time duration to the next connection (TDNC) (see [0086] to [0093] and [0130] to [0145]).

As to claim 33, Ishida discloses updating, by a client, the new access log approximately every new variable time period (VTP) (see [0086] to [0093] and [0130] to [0145]).



***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 3-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishida in view of Coddington et al., US pat. No.5,410,343 (hereafter Coddington).

As to claims 3-6, Ishida's teachings still applied as in item 2 above. Ishida does not disclose using a set-top box, a video home server, a pay-per-view video server and a video-on-demand server. However, Coddington discloses using a set-top box, a video home server, a pay-per-view video server and a video-on-demand server (see abstract, figs.1, 2, col.5 line 8 to col.6 line 42 and col.9 line 38 to col.10 line 61). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Coddington's teachings into the computer system of Ishida to distribute data

information in a communications network because it would have provided direct data transfer between the customer's premises and the associated Video Information Provider to support interactive video programming and presentations in a communications network (see Coddington's col.10 lines 1-39).

6. Claims 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ishida in view of Elgamal, US pat. No.5,671,279 (hereafter Elgamal).

As to claim 8, Ishida's teachings still applied as in item 2 above. Ishida does not disclose using a Secure Authenticated Channel (SAC) connection. However, Elgamal disclose using a Secure Authenticated Channel (SAC) connection (providing a secure authenticated channel for all communications between the Merchant and the Acquirer Gateway to secure all messages exchanged properly, see abstract, fig.1, col.20 line 59 to col.21 line 17). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Elgamal's teachings into the computer system of Ishida to provide secure data transactions because it would have provided a secure communications between the merchant and Gateway and to protect account information from the merchant in the Internet (see Elgamal's col.20 lines 52-64).

***Other prior art cited***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Sekiguchi, US pat. No.6,711,687.

- b. Harris, US pat. No.6,711,610.
- c. Basu et al., US pat. No.6,868,439.

### ***Conclusion***

- 8. Claims 1-33 are rejected.
- 9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khanh Dinh whose telephone number is (571) 272-3936. The examiner can normally be reached on Monday through Friday from 8:00 A.m. to 5:00 P.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung, can be reached on (571) 272-3939. The fax phone number for this group is (703) 872-9306.

*A shortened statutory period for reply is set to expire THREE months from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned (35 U. S. C . Sect. 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(A).*

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you

Art Unit: 2151

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Khanh Dinh  
Patent Examiner  
Art Unit 2151  
6/23/2005